REMARKS

The present amendment is responsive to the Office Action issued December 1, 2005. A petition for a one-month extension of time is submitted herewith. Claims 1, 11, 21 and 31 have been amended to include the limitations of claims 2, 12, 22 and 32, respectively. Claims 2, 12, 22 and 32 have been canceled. New claims 45-46 have been added. No new matter has been added by the amendments or the new claims. Support for the amendments and new claims may be found, by way of example only, in specification pages 5-20. Therefore, claims 1, 6-11, 16-21, 26-31, and 36-46 are now presented for consideration in view of the following remarks.

As an initial matter, applicants note that claims 41-44, which depend, respectively, from independent claims 1, 11, 21 and 31 were added in the amendment dated July 20, 2005. However, claims 41-44 were not addressed in the Office Action of December 1, 2005.

Claims 1-2, 6-12, 16-22, 26-32, and 36-40 were rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 5,894,516 ("*Brandenburg*") in view of U.S. Patent No. 6,049,671 ("*Slivka*") and U.S. Patent No. 5,790,753 ("*Krishnamoorthy*"). Applicants respectfully traverse the rejection.

As discussed in amendments to previous Office Actions, *Brandenburg* discloses a broadcast software distribution system that can transmit data from a software distribution center ("SDC") to a target computer via a satellite link. *Brandenburg* states the "encryption key is then itself encrypted using a target computer identification code, and the encrypted encryption key is loaded onto the target computer." (Abstract.)

The Office Action acknowledges that *Brandenburg* does not employ unique terminal identification information that is selected in a manner unrelated to authentication data, as

12

required by independent claims 1, 11, 21 and 31. *Slivka* is relied on to remedy this deficiency.

Slivka, as discussed in the previous amendment, "relates to a system for automatically identifying software that may be appropriate for installation on a computer and for making that software available to that computer." (Col. 1, lns. 11-24.) *Slivka* goes on to state that an "encryption scheme may also be used to permit safe transfer of the software to the user computer." (Col. 9, lns. 24-25.)

Applicants maintain that the combination of *Brandenburg* and *Slivka* is improper because the combination does not result in the claimed invention and there is no teaching, suggestion, or motivation to combine the references as proposed by the Examiner to arrive at the claimed invention.

As discussed in the previous amendment, the technical teachings of *Brandenburg* and *Slivka* are such that their combination would not result in the claimed invention, even if combined. *Brandenburg* neither teaches nor suggests unique terminal identification information that is selected in a manner unrelated to the authentication data. Instead, the broadcast software distribution system of *Brandenburg* encrypts its software encryption key for the ordered software package using the identification code of the target computer.

While *Brandenburg* provides "a unique method, apparatus, and article of manufacture for <u>broadcasting encrypted software</u> to a target computer," *Slivka* does not address broadcasting of software at all. (*Brandenburg*, col. 1, lns. 57-59, emphasis added.) Unlike *Slivka*, *Brandenburg's* encryption scheme appears tailored for the problem of broadcasting software updates. (*See* col. 1, lns. 46-51.)

In contrast, *Slivka* employs RSA encryption, which "is completed with a 1024-bit private key known only to the software

distributor ... The distributed is decrypted using a published public RSA decryption key." (Col. 17, 11. 16-21.)

There is no teaching or suggestion in *Brandenburg*, *Slivka* or the other art of record as to how *Brandenburg* could be redesigned to incorporate the RSA algorithm of *Slivka* while still achieving its goals of broadcast downloading of software. As discussed above, *Brandenburg* uses the identification code of the target computer to both encrypt and decrypt the encryption key. It does not appear that the RSA algorithm mentioned by *Slivka* could simply be implemented in lieu of *Brandenburg's* recited encryption scheme as suggested in the Office Action. Finally, it is not even clear that such a combination is feasible based upon the broadcast system of *Brandenburg*.

Second, one skilled in the art would not have been motivated to combine the teachings of *Brandenburg* and *Slivka*. The asserted motivation supplied by the Office Action, namely a more robust encryption process, appears to be irrelevant given the broadcast system and specific teachings of *Brandenburg*. *Brandenburg* utilizes a <u>unique</u> computer identifier code <u>associated with the computer</u> to both encrypt and decrypt an encryption key, which teaches away from using a random number generator as suggested in the Office Action. *Slivka* utilizes the RSA encryption algorithm to safely transfer software to a user's computer. It is not clear or obvious to use the RSA algorithm in broadcast download of software to multiple terminals, such as in a satellite set top box system. Rather, the teachings of *Slivka* go against the teachings of *Brandenburg*.

The fact that a prior art process or device could be modified so as to produce the claimed invention is not a basis for an obviousness rejection unless the prior art suggests the desirability of such modification. *In re Gordon*, 733 F.2d 900, 221 U.S.P.Q. 1125 (Fed. Cir. 1984). As stated in *In re Oetiker*, 997 F.2d 1443, 1447, 24 U.S.P.Q.2d 1443 (Fed. Cir. 1992):

> There must be some reason, suggestion, or motivation found in the prior art whereby a person of ordinary skill in the field of the invention would make the combination. That knowledge cannot come from the applicant's invention itself.

There is simply no teaching or motivation in the cited art to reengineer the *Brandenburg* system using an incompatible encryption scheme as disclose in *Slivka* in order to arrive at the elements recited in claims 1, 11, 21 and 31. The aforementioned arguments against the improper combination of *Brandenburg* and *Slivka* were presented in the previous amendment. However, the pending Office Action does not address the arguments at all, instead maintaining that it would be desirable to modify *Brandenburg* to utilize the RSA algorithm of *Slivka*.

Notwithstanding the aforesaid deficiencies of *Brandenburg* and *Slivka*, independent claims 1, 11, 21 and 31 have also been amended to include the limitations of dependent claims 2, 12, 22 and 32, respectively, to further clarify the claimed invention.

Claims 2, 12, 22 and 32 were rejected in the Office Action because *Brandenburg* discloses "the target computer 18 requesting new versions of software applications that have already been downloaded." (Office Action, numbered section 2 at pg. 5.) According to the portion of *Brandenburg* cited in the Office Action, "As an option, the receiver could be set up to look for and download a specific list of ordered products, or specific versions of a product. For example, a user may want to always download new versions of products that were already installed so that the user always has the latest version of the software product." (Col. 4, ll. 8-14.)

The amended independent claims are specific as to how transfer requests are implemented. Such limitations are simply not present in *Brandenburg*. For instance, amended claim 1 recites "transmitting from said one receiving terminal to said

transmission apparatus a transfer request based on said update program and said unique terminal information; and supplying data responsive to said transfer request from said transmission apparatus to said one receiving terminal based on said unique terminal information." Amended claims 11, 21 and 31 include similar limitations. The cited portion of *Brandenburg* is simply devoid of such teachings. The other art of record fails to overcome the deficiencies of *Brandenburg*.

In view of the foregoing, it is respectfully submitted that claims 1, 11, 21 and 31 patentably distinguish over *Brandenburg* and *Slivka*, both individually and in the combination that the Examiner suggests can be made therefrom. Therefore, applicants respectfully request reconsideration and allowance of independent claims 1, 11, 21 and 31.

Furthermore, claims 6-10, 16-20, 6-30, and 36-44 depend from independent claims 1, 11, 21 and 31, respectively, and contain all of the limitations thereof as well as other limitations that are neither disclosed nor suggested by the prior art of record. Accordingly, applicants submit that the subject dependent claims are likewise patentable.

As indicated above, new claims 45 and 46 have been added. Claim 45 is for a method of transmitting data between a provider device and one of a plurality of client devices remote from the provider device. By way of example only, the claim recites, among other limitations, "the provider device assigning a MAC address to a receiving device coupled to the first client device, the MAC address being a unique address for use with a receiver device and being unrelated to the recognition data of the first client device; the provider device generating a unique key ID based on the MAC address; transmitting a software application, a download application and the unique key ID from the provider device to the first client device" and "if the unique key ID is validated: transferring the software

16

application to the receiver device; retrieving the MAC address from the unique key ID; and transferring the MAC address to the receiver device for use as a new address of the receiver device."

Claim 46 is for a system having a provider device, a plurality of client devices and a plurality of receiver devices. The claim recites, among other limitations, "wherein the provider device is operable to authenticate the recognition data of the first client device, to assign a unique MAC address unrelated to the recognition data of the first client device to the first receiver device, to generate a unique key ID based on the MAC address and to transmit a software application, a download application and the unique key ID to the first client device, and wherein the client device is operable to execute the download application to identify the unique key ID, to validate the unique key ID, and, if the unique key ID is validated, to transfer the software application to the receiver device, to retrieve the MAC address from the unique key ID, and to transfer the MAC address to the receiver device for use as a new address of the receiver device."

Neither *Brandenburg*, *Slivka*, *Krishnamoorthy* nor the other art of record teaches or suggests, either alone or in combination, the limitations of claims 45 and 46. Accordingly, applicants submit that independent claims 45 and 46 are patentable as well.

As it is believed that all of the rejections set forth in the Office Action have been fully met, favorable reconsideration and allowance are earnestly solicited.

If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that he telephone applicant's attorney at (908) 654-5000 in order to overcome any additional objections which he might have. If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: March 16, 2006   Respectfully submitted,
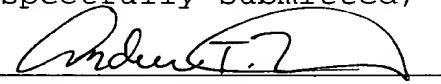
By _____
Andrew T. Zidel
Registration No.: 45,256
LERNER, DAVID, LITTENBERG,
  KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorney for Applicant

639536_1.DOC

18